HR
WSD Personnel

SAP Business Intelligence Reporting

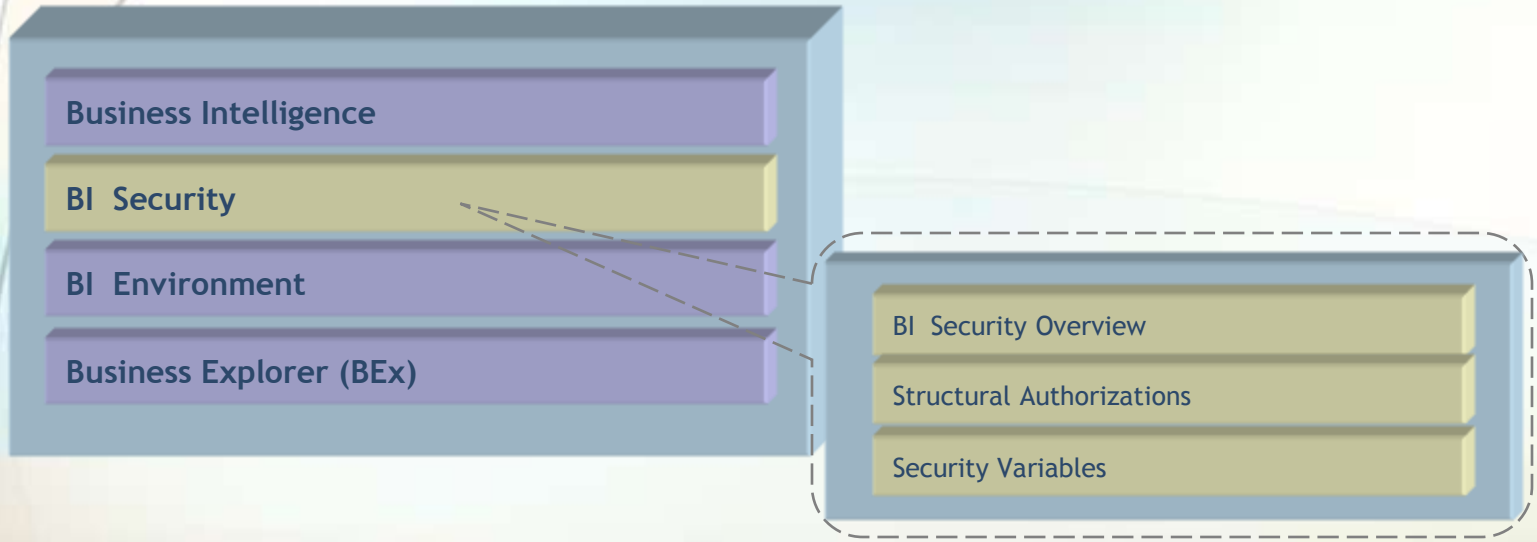
BI Security

Washington State HRMS Business Intelligence (BI)
BI Power User Workshop Materials

General Topics – BI Power User

BI Security

The following section provides an overview of BI Security.



BI Security Overview

The ability to access BI reports, specific functions, and data within the BI environment is controlled by HRMS BI Security:

1. BI User Role – The ability to access specific functions in BI is controlled through roles. Agency HRMS BI users will be mapped to either a "BI End User" or "BI Power User" role. All BI users can access reports via the HRMS Portal. Only Power Users can develop ad hoc queries against data available within the BI structures.
2. BI InfoProvider Role – The ability to access BI data structures (InfoProviders) is controlled by a BI InfoProvider Role. Agency HRMS BI users will be mapped to either an "HR/Payroll/Time data" – or- "HR/Payroll/Time with Financial data" – or – "Financial data only" InfoProvider Role.
3. BI Data Security – The ability to access report results is controlled through the organization structure within the security and role mapping setups. BI data structures apply an additional level of data security for specific values such as SSN, Name, etc.

BI User Role and BI InfoProvider Role are discussed in more detail in the BI Concepts module of the BI Self-Paced Learning Materials.

Structural Authorizations

BI Data Security

BI Data Security is based on Structural Authorizations.

- Structural Authorizations are defined in HRMS (SAP R/3) and are loaded to the BI on a nightly basis. Structural Authorizations restrict the display of data based on the user's organization structure within the security and role mapping setups.
- Some InfoObjects within BI are considered confidential (for example, SSN and Name). BI Security will check Structural Authorizations to ensure the user receives results for only the data they have access to.

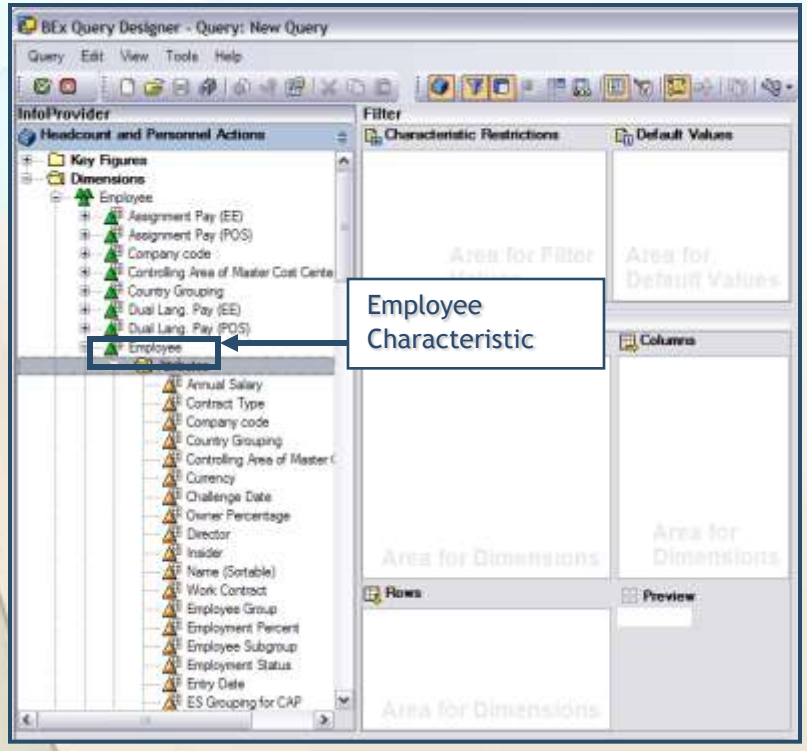
Continued…

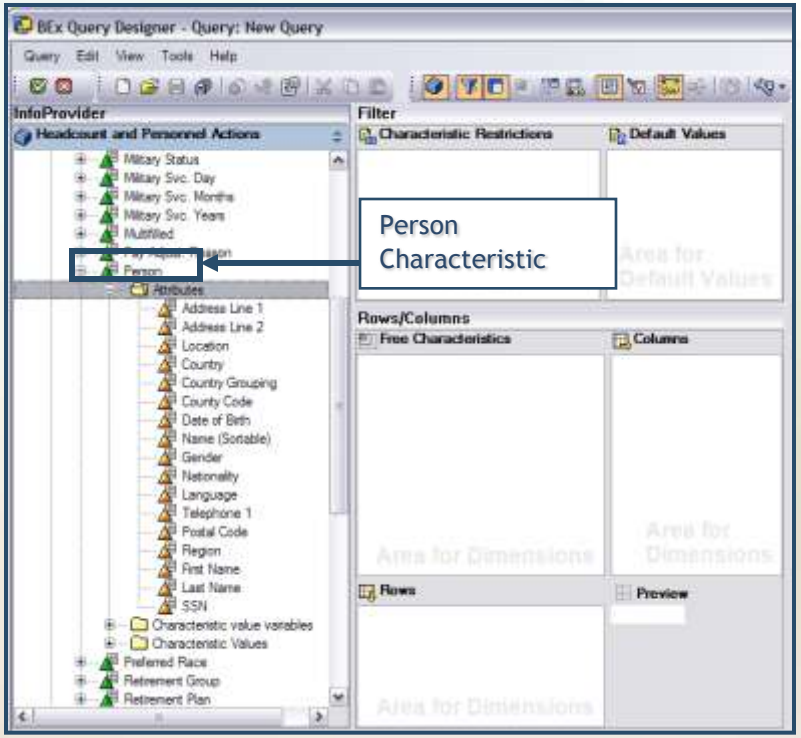
Structural Authorizations, Cont…

In BI , there are two characteristics identified as confidential InfoObjects:

1. Employee (0EMPLOYEE)
2. Person (0PERSON)

BI security will check Structural Authorizations when these two characteristics are included in queries and reports. This will ensure the user receives results for only the data they have access to.

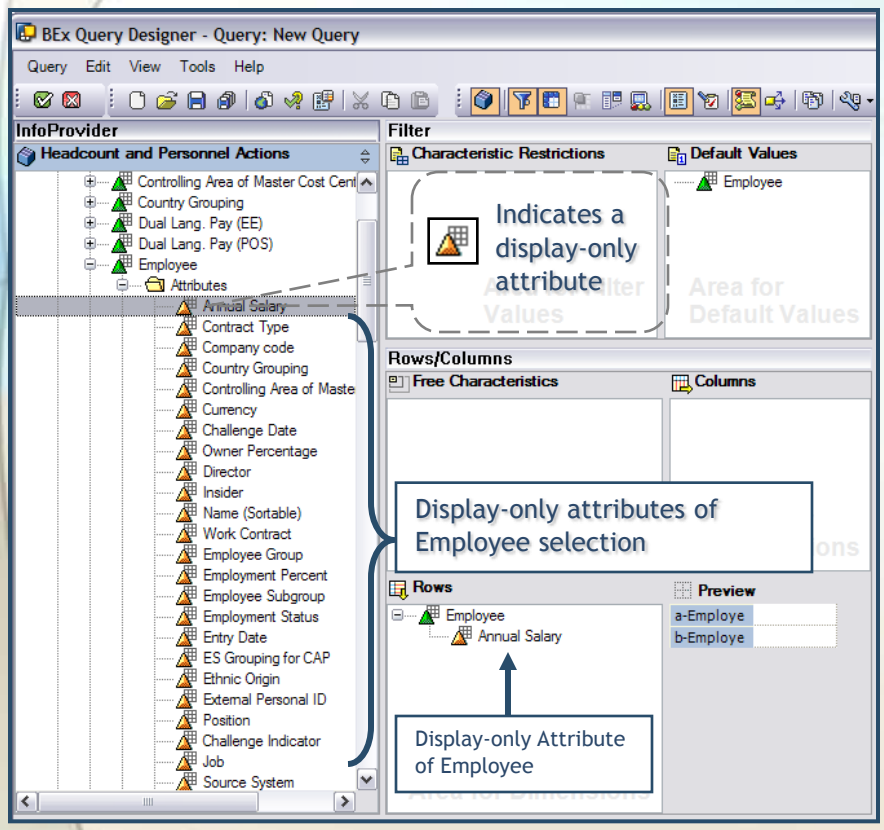




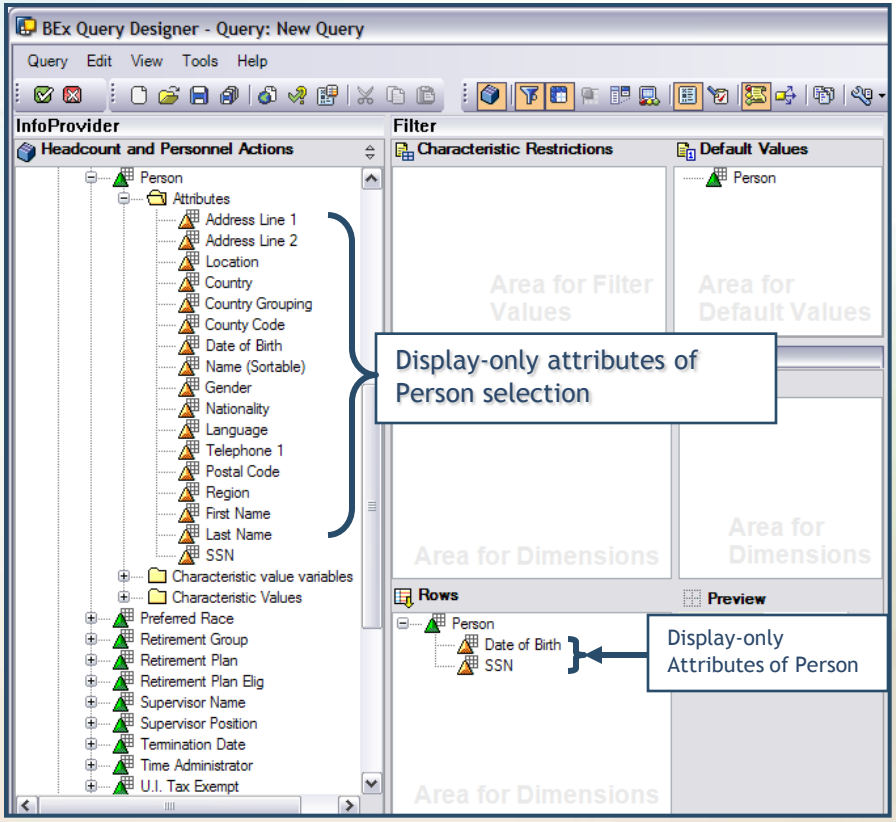
Continued…

Structural Authorizations, Cont…

Employee and Person have display-only attributes that are located in the Attributes folder of the characteristic. These display-only attributes can only be included in a query or report if Employee or Person characteristics are also included.



Display-only attributes of Employee



Display-only attributes of Person

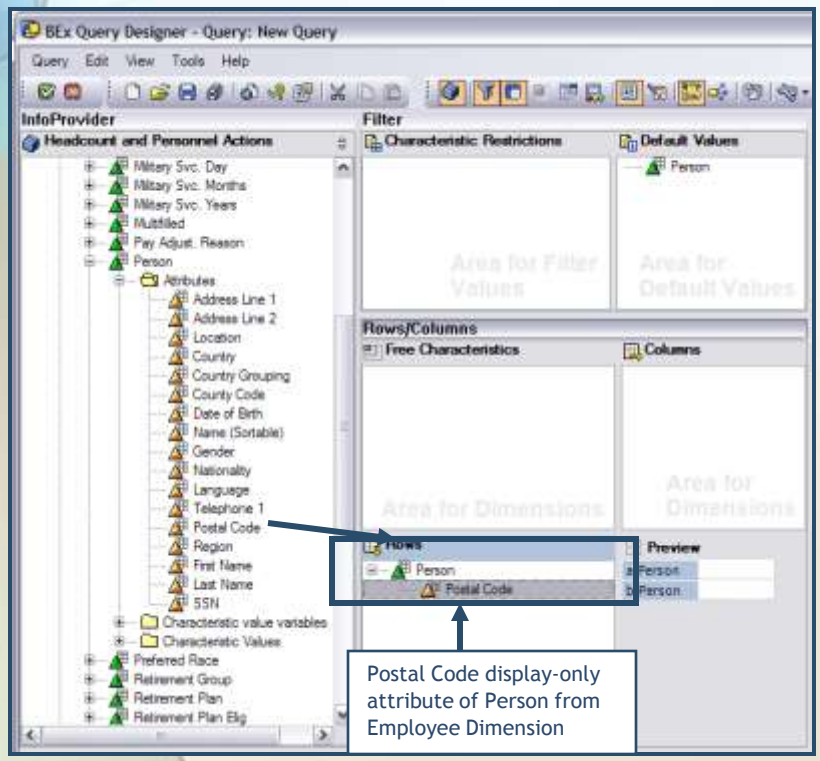
Continued…

Structural Authorizations, Cont…

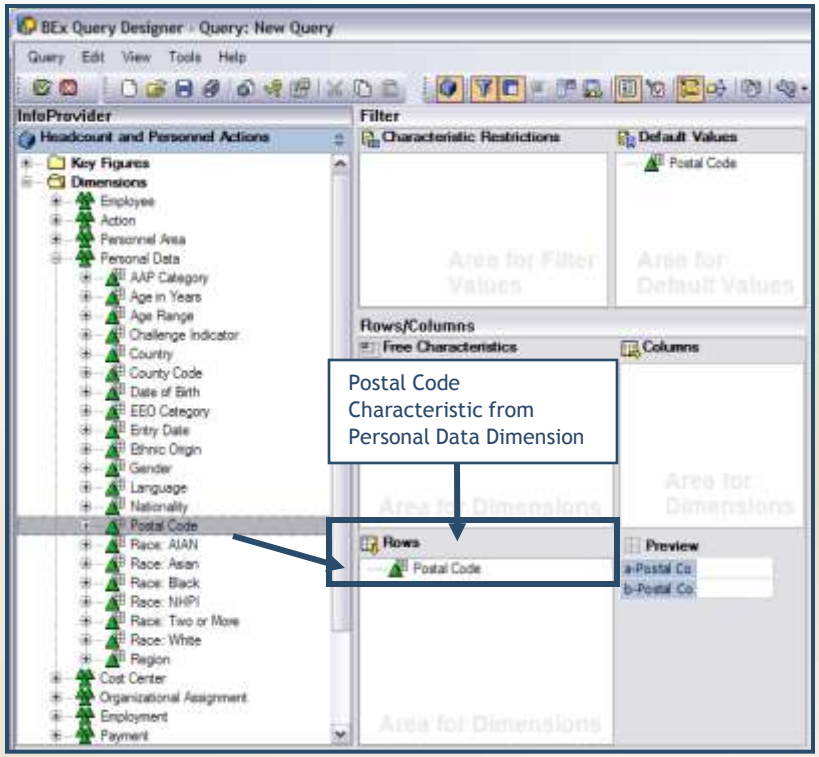
Some display-only attributes of Employee and Person are not necessarily confidential. For example, Postal Code is generally not a confidential field.

In Example 1 below, Postal Code is a display-only attribute of Person. Since Postal Code must be included with the Person characteristic, BI Security will check Structural Authorizations.

In Example 2 below, Postal Code is not a display-only attribute of Person. Postal Code is a characteristic. Since Postal Code is a characteristic, BI Security will not check Structural Authorizations. Users can report on Postal Codes statewide.



Example 1: Postal Code Display-only attribute – Checks Structural Authorizations



Example 2: Postal Code Characteristic – Does not check Structural Authorizations

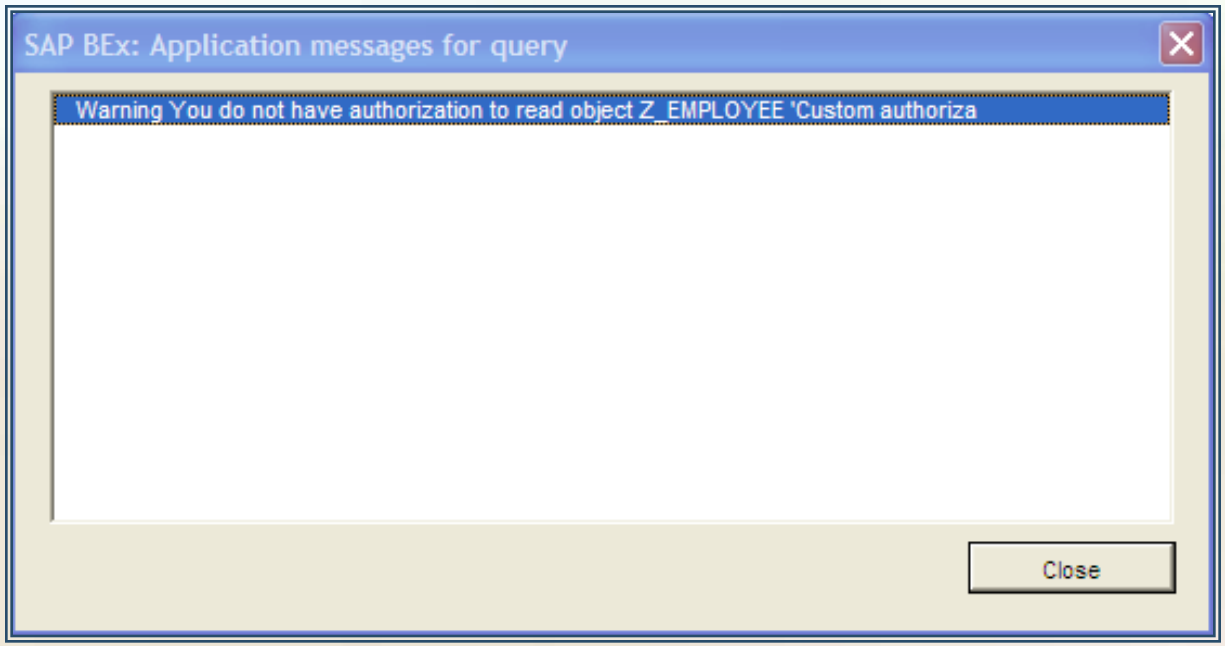
Security Variables

Security Variables are variables in a query or report that check Structural Authorizations. If Employee or Person characteristics are included in a query or report, a Security Variable must also be included.

When a Security Variable is included with the Employee or Person characteristics, BI Security will check Structural Authorizations. This will ensure the user receives results for only the data they have access to.

If a Security Variable is not included with the Employee or Person characteristics, BI Security will return an authorization error for users who do not have statewide access.

An example of the authorization error is displayed below:



Continued...

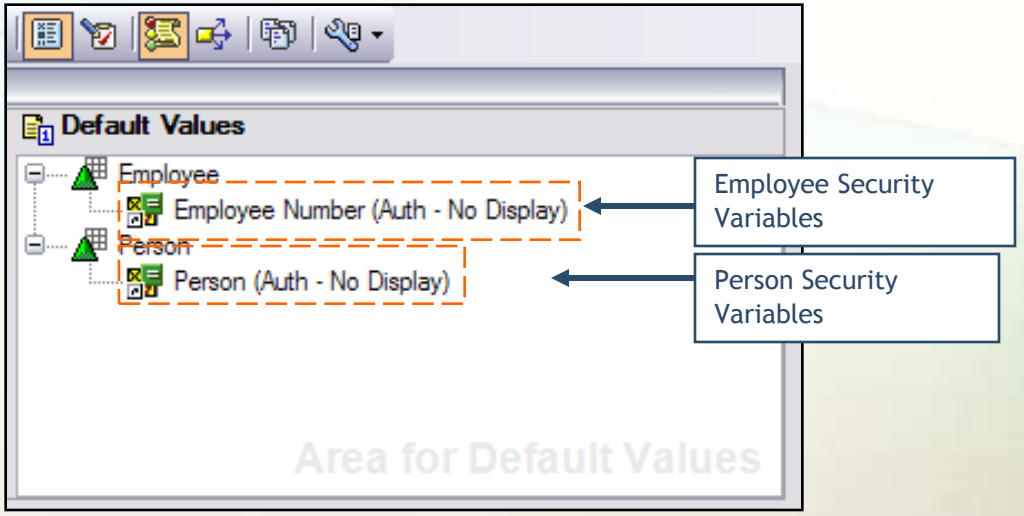
Security Variables, Cont…

Employee and Person have two types of Security Variables:

1. Display: Prompts users to select an Employee or Person prior to running the query.
2. No Display: Does not prompt users to select an Employee or Person prior to running the query. Automatically returns data the user has security access to.

Security Variables for Employee and Person include:

- Employee (0EMPLOYEE):
  - No Display: "Employee Number (Auth – No Display)"
- Person (0PERSON):
  - No Display: "Person (Auth) No Display"

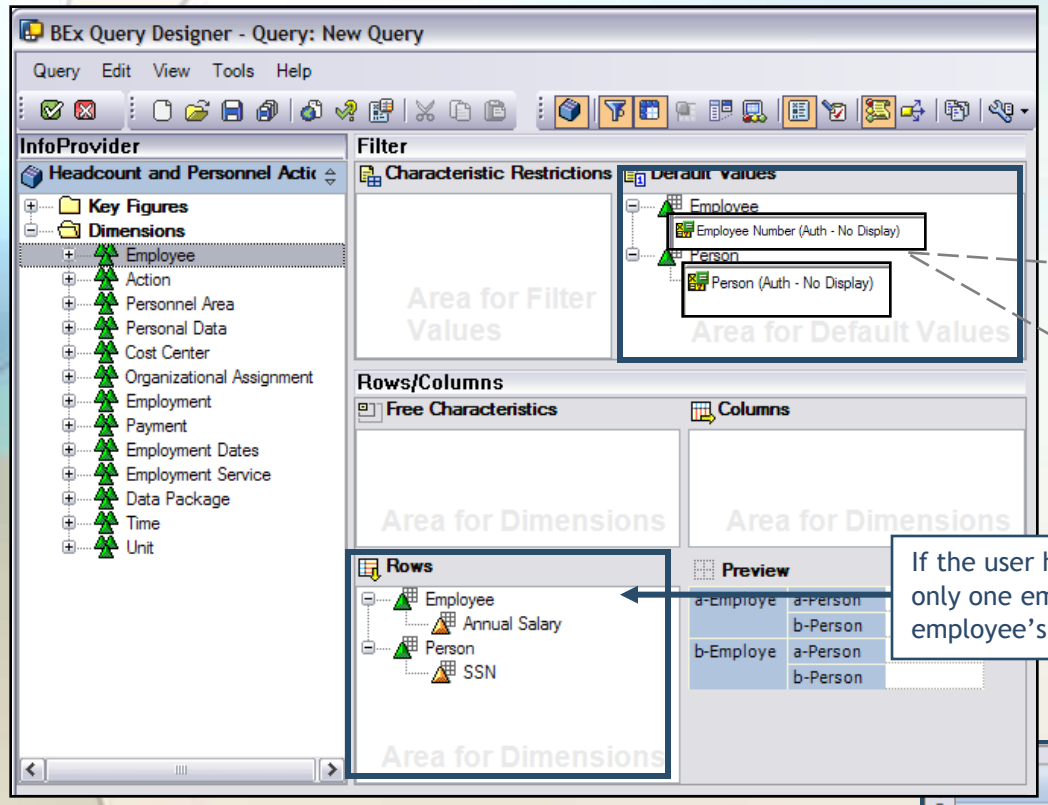


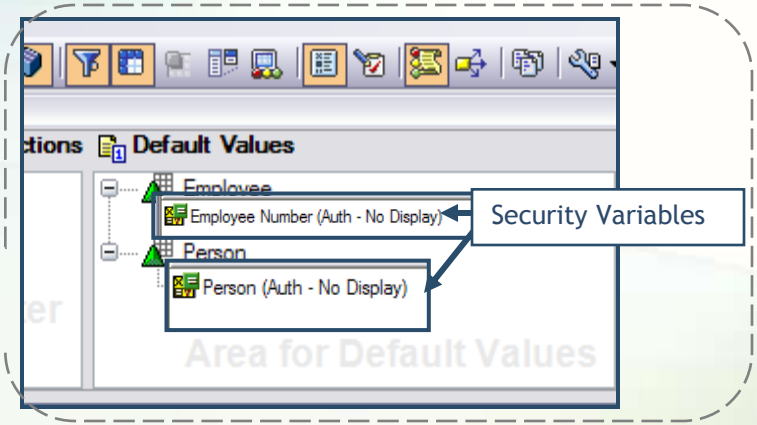
If a Display Security Variable is included in a query or report and the user running the query manually adds an employee they do not have access to in the variable selection, they will receive an authorization error. Structural Authorizations are checked after the Variable selection screen to ensure any new employees that may have been added to the employee list are in the users Structural Authorizations.

Continued…

Security Variables, Cont…

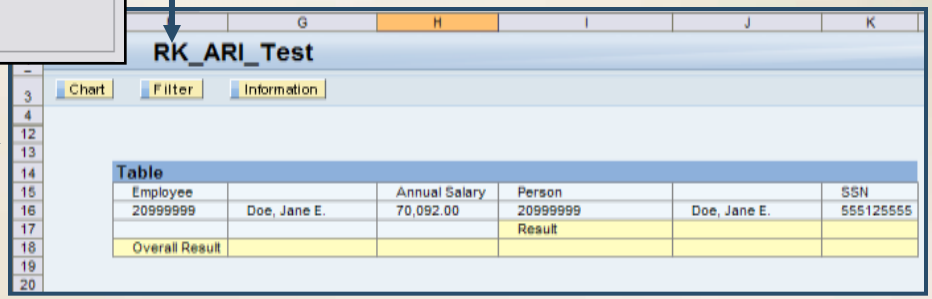
The example below uses a new query to show the results of using Employee and Person characteristics with Security Variables.





If the user has authorization to view only one employee, only one employee's data will be displayed.

Sample of an ad hoc query with Confidential InfoObjects and Security Variables



Result: Return data for employees the user has access to